

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-8617

(43) 公開日 平成11年(1999) 1月12日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 9/12		H 0 4 L 9/00	6 3 1
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 G
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B
12/54		11/20	1 0 1 B

審査請求 有 請求項の数 3 O L (全 7 頁) 最終頁に続く

(21) 出願番号 特願平9-160989

(22) 出願日 平成9年(1997) 6月18日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 佐藤 太郎

東京都港区芝五丁目7番1号 日本電気株式会社内

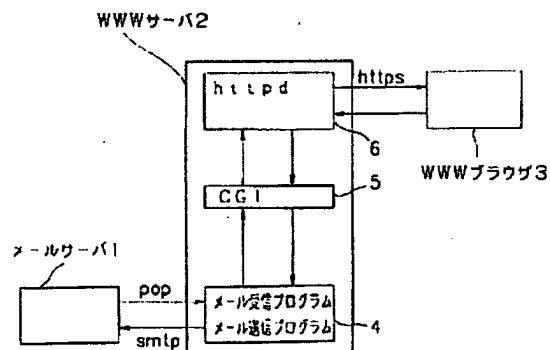
(74) 代理人 弁理士 丸山 隆夫

(54) 【発明の名称】 電子メールの暗号化システム及び暗号化方法

(57) 【要約】

【課題】 電子メールの送受信を安全に行い、かつ、効率的に行うことの可能な電子メールの暗号化システム及び暗号化方法を提供する。

【解決手段】 少なくとも1以上の端末に備えられたWWWブラウザ3が、電子メールをhttpsにより暗号化して送信し、かつ、受信したhttpsにより暗号化された電子メールを復号化して画面に表示させ、メールサーバ1が、受信した電子メールを蓄積し、WWWサーバ2が、端末から送信されたhttpsにより暗号化された電子メールを復号化してメールサーバ1に送信し、かつ、メールサーバ1から送信された電子メールをhttpsにより暗号化してWWWブラウザ3が備えられた端末に送信する。



【特許請求の範囲】

【請求項1】 電子メールをhttpsにより暗号化して送信し、かつ、受信したhttpsにより暗号化された電子メールを復号化して画面に表示させるWWWブラウザを備えた少なくとも1以上の端末と、受信した電子メールを蓄積するメールサーバと、前記端末から送信されたhttpsにより暗号化された電子メールを復号化して前記メールサーバに送信し、かつ、前記メールサーバから送信された電子メールをhttpsにより暗号化して前記端末に送信するWWWサーバとを有することを特徴とする電子メールの暗号化システム。

【請求項2】 前記WWWサーバが、前記端末から送信されたhttpsにより暗号化された電子メールを復号化し、かつ、電子メールをhttpsにより暗号化して出力するhttpdと、前記httpdにより復号化された電子メールをメールサーバに送信すると共に、前記メールサーバから送信された電子メールを受信するCommon Gateway Interfaceとを有することを特徴とする請求項1記載の電子メールの暗号化システム。

【請求項3】 端末に備えられたWWWブラウザにより、電子メールをhttpsにより暗号化してWWWサーバに備えられたhttpdに送信する工程と、前記暗号化された電子メールをWWWサーバに備えられたhttpdにより復号化し、Common Gateway Interfaceに送信する工程と、前記Common Gateway Interfaceに送信された電子メールを、Common Gateway Interfaceに備えられたメール送信プログラムに従ってメールサーバに送信する工程とを備えた、端末からメールサーバへの電子メール送信工程と、前記Common Gateway Interfaceが、Common Gateway Interfaceに備えられたメール受信プログラムに従ってメールサーバから電子メールを受信し、該受信した電子メールを前記httpdに出力する工程と、前記httpdが、httpdに出力された電子メールを、httpsにより暗号化してWWWブラウザが備えられた端末に送信する工程と、前記暗号化された電子メールを受信した端末が、前記WWWブラウザにより受信した電子メールを復号化して表示する工程とを備えた、メールサーバから端末への電子メール送信工程とを有することを特徴とする電子メールの暗号化方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、電子メールの暗号化システム及び暗号化方法に関し、特に端末に備えられたWWWブラウザにより電子メールを送受信する場合の

電子メールの暗号化システム及び暗号化方法に関する。

【0002】

【従来の技術】 現在、インターネットの発展に伴い、そのネットワークにおいて取り扱われるデータに対するセキュリティの向上が重要な課題となっている。

【0003】 特に、World Wide Web（以下、単にWWWと記す。）上での電子メール送受信方式は、メールサーバに電子メールを蓄積することができ、利用者の都合に合わせて電子メールの送受信を行えるため、その簡便さから広く利用され、それに伴い、電子メールを取り扱う際の、秘密保持やデータの複製防止等のセキュリティの向上が必要となっている。

【0004】 そのため、従来では、電子メールを暗号化して送受信を行う方式が提案されている。

【0005】 従来、この種の電子メールを暗号化しての送受信は、電子メールの内容を、送信者及び受信者以外の第三者に読まれることを防ぐために用いられている場合が多い。

【0006】 例えば、電子メールの暗号化送受信方法の一例として、特開平8-251156号公報に開示された、「電子メール暗号化方法及び暗号化システム」について、以下に説明する。

【0007】 この公報に記載された電子メールの暗号化送受信方法は、通信ネットワークの各利用者のそれぞれが、各々の鍵情報を作成し、公開鍵を公開することによって暗号化を可能にし、セキュリティの向上を図るものである。

【0008】 具体的には、前準備として各利用者が各々の鍵情報を専用のソフトウェアで作成し、あらかじめセンタに登録しておく。送信する電子メールを暗号化する際は、電子メール本文をデータ鍵により暗号化し、このデータ鍵をマスタ鍵により暗号化し、この2つの暗号化されたデータを電子メールデータとして送信する。この2つの暗号化されたデータを受信した端末は、暗号化されたデータ鍵のデータをマスタ鍵を用いて復号化し、この復号化されたデータ鍵を用いて暗号化された電子メールデータを復号化し、電子メールの受信を行う。

【0009】 従って、この従来の電子メールの暗号化送受信方法によれば、電子メールの偽造や複製等を有効に防止し、安全性の高い電子メール暗号化方法を提供することができるとしている。

【0010】

【発明が解決しようとする課題】 しかしながら、上述の従来の電子メールの暗号化送受信方法においては、送受信を行う端末を特定し、この特定された端末間で鍵を共有する必要があるため、個々の端末において鍵情報を作成し、かつ、この鍵情報を公開しなければならず、電子メールの暗号化を行う際の効率が低減すると共に、ネットワークの安全性にも支障をきたすという問題点を有する。

【0011】また、上述のような従来の電子メールの暗号化システムにおいては、電子メールの暗号化及び復号化を、個々の端末上において実行しているため、個々の端末は、それぞれ暗号化及び復号化のためのハードウェアやソフトウェア等を具備しなければならず、暗号化及び復号化を行うためのその端末のコストが上昇するという問題点を有する。

【0012】本発明は、上記事情に鑑みなされたもので、電子メールの送受信を安全に行い、かつ、効率的に行うことの可能な電子メールの暗号化システム及び暗号化方法を提供することを目的とする。

【0013】

【課題を解決するための手段】請求項1記載の発明は、電子メールをhttpsにより暗号化して送信し、かつ、受信したhttpsにより暗号化された電子メールを復号化して画面に表示させるWWWブラウザを備えた少なくとも1以上の端末と、受信した電子メールを蓄積するメールサーバと、前記端末から送信されたhttpsにより暗号化された電子メールを復号化して前記メールサーバに送信し、かつ、前記メールサーバから送信された電子メールをhttpsにより暗号化して前記端末に送信するWWWサーバとを有することを特徴とする。

【0014】従って、この発明によれば、端末とメールサーバとの間において電子メールの送受信を行う場合、WWWサーバと端末との間においては、その電子メールが、hyper text transfer protocol（以下、単にhttpと記す。）におけるセキュリティ強化型のプロトコルである、httpsにより暗号化されていることから、安全に電子メールの送受信を行うことができる。

【0015】また、電子メールを暗号化する際には、WWWサーバ及びWWWブラウザがhttpsによる暗号化を行うので、個々の端末の鍵情報の作成や、その公開等は必要ではないので、電子メールの暗号化の効率を向上させることができ、その安全性を向上させることができる。

【0016】また、端末に備えられたWWWブラウザにより電子メールに対する暗号化及び復号化を行って送受信を行うため、電子メールを暗号化及び復号化して送受信する際に新たな部材を設ける必要はない。

【0017】また、端末の利用者はWWWサーバからhttpsにより暗号化され転送された電子メールの内容をWWWブラウザが備えられた端末の画面において読むことができ、逆にWWWブラウザが備えられた端末の画面で記入した電子メールの内容をhttpsにより暗号化してWWWサーバに転送することができるので、httpsにより暗号化された電子メールの送受信は、インターネット上の任意の場所の端末において行うことができる。

【0018】請求項2記載の発明は、請求項1記載の発

明において、前記WWWサーバが、前記端末から送信されたhttpsにより暗号化された電子メールを復号化し、かつ、電子メールをhttpsにより暗号化して出力するhttpdと、前記httpdにより復号化された電子メールをメールサーバに送信すると共に、前記メールサーバから送信された電子メールを受信するCommon Gateway Interfaceとを有することを特徴とする。

【0019】従って、この発明によれば、請求項1記載の発明の作用が得られると共に、電子メールの暗号化及び復号化をWWWサーバに備えられた、httpサーバである、httpd(hyper text transfer protocol demon)が行ない、メールサーバとの間での電子メールの送受信をCommon Gateway Interface（以下、CGIと言う。）が行い、同様に、端末では、端末に備えられたWWWブラウザが電子メールの暗号化及び復号化を行っているため、暗号化及び復号化を行うためのhttpsに対応したWWWブラウザであれば電子メールの暗号化及び復号化を行えるため、特別な部材を用いることなく電子メールの暗号化及び復号化を行うことができる。

【0020】請求項3記載の発明は、端末に備えられたWWWブラウザにより、電子メールをhttpsにより暗号化してWWWサーバに備えられたhttpdに送信する工程と、前記暗号化された電子メールをWWWサーバに備えられたhttpdにより復号化し、Common Gateway Interfaceに送信する工程と、前記Common Gateway Interfaceに送信された電子メールを、Common Gateway Interfaceに備えられたメール送信プログラムに従ってメールサーバに送信する工程とを備えた、端末からメールサーバへの電子メール送信工程と、前記Common Gateway Interfaceが、Common Gateway Interfaceに備えられたメール受信プログラムに従ってメールサーバから電子メールを受信し、該受信した電子メールを前記httpdに出力する工程と、前記httpdが、httpdに出力された電子メールを、httpsにより暗号化してWWWブラウザが備えられた端末に送信する工程と、前記暗号化された電子メールを受信した端末が、前記WWWブラウザにより受信した電子メールを復号化して表示する工程とを備えた、メールサーバから端末への電子メール送信工程とを有することを特徴とする。

【0021】従って、この発明によれば、端末からメールサーバへ電子メールを送信する場合は、端末に備えられたWWWブラウザにより電子メールをhttpsにより暗号化してWWWサーバに送信し、WWWサーバに備えられたhttpdはこの電子メールを復号化し、Co

Common Gateway Interfaceがこの復号化された電子メールをメール送信プログラムに基づいてメールサーバに送信し、また、メールサーバから端末への電子メールを送信する場合には、Common Gateway Interfaceがメール受信プログラムに基づいてメールサーバから電子メールを受信し、この受信した電子メールをhttpdに送信し、httpdがこの送信された電子メールをhttpsにより暗号化してWWWブラウザに送信するので、従来技術のように、電子メールの暗号化及び復号化を行う際に、個々の端末において鍵情報を作成するという手間を省くことができると共に、その鍵情報を公開する必要もないため、その安全性を向上することができる。

【0022】また、電子メールの暗号化及び復号化が、httpsにより行われているため、一般的なWWWブラウザであれば電子メールの暗号化及び復号化を行うことができ、電子メールの暗号化及び復号化のための特別な部材を必要としないので、電子メールの暗号化及び復号化を行う際のコストの上昇を抑えることができる。

【0023】

【発明の実施の形態】次に、本発明に係る電子メールの暗号化システム及び暗号化方法の実施形態について図面を参照して詳細に説明する。

【0024】図1に、本発明に係る電子メールの暗号化システムの一実施形態の構成の概念図を示す。この図1に示されるように、この電子メールの暗号化システムは、受信した電子メールを蓄積するメールサーバ1と、メールサーバ1から電子メールを受信し、WWWブラウザ3からhttpsにより暗号化された電子メールを受信するWWWサーバ2と、メールサーバ1に送受信する電子メールを表示するためのWWWブラウザ3とから構成されている。

【0025】また、上述のWWWサーバ2は、メール受信プログラム及びメール送信プログラム4を有するCGI(Common Gateway Interface)5と、CGI5との間で電子メールの送受信を行い、WWWブラウザ3との間でhttpsにより暗号化された電子メールの送受信を行うhttpd6とから構成される。ここで、以下に述べるhttpsは、Open Systems Interconnection(開放型システム間相互接続)におけるSecurity Socket Layer(以下、単にSSLと記す。)を用いる。

【0026】WWWサーバ2に備えられているhttpd6は、一般に広く用いられているhttps(SSL)を利用可能なものであるならば、どのような種類のものを用いても良い。また、通常の方法でhttpsにより、WWWブラウザ3との間において暗号化通信を行う。

【0027】WWWブラウザ3は市販されているhtt

ps(SSL)対応のものであるならばいずれでも良く、またインターネット上の特定の場所の端末に備えられている必要はない。従って、WWWブラウザ3はhttpd6と通信することが可能な任意の場所の端末であれば良い。

【0028】メールサーバ1はWWWサーバ2と同一のコンピュータ上にあり、その機能は一般に広く用いられているUNIX(登録商標)のsendmailと何ら変わるところはない。すなわち、メールサーバ1には、電子メールの暗号化のための特別な部材を付与する必要はない。

【0029】次に、この図1を参照して、本発明に係る電子メールの暗号化方法について説明する。

【0030】WWWブラウザ3から、メールサーバ1に蓄積された電子メール購読の要求がhttpd6に送られると、httpd6は、CGI5が有するメール受信プログラム4にメール受信要求を出力する。

【0031】メール受信要求を受けたメール受信プログラム4は、メールサーバ1にメール受信要求を出力する。メール受信要求を受けたメールサーバ1は、要求された電子メールをCGI5に送信する。そして、CGI5に備えられたメール受信プログラム4は、通常のpopプロトコルにより電子メールを受信する。この受信した電子メールをCGI5がhttpd6に出力する。

【0032】httpd6は電子メールをhtml(hypertext markup language)に成形した上で、httpsにより暗号化してWWWブラウザ3に送信する。

【0033】一方、WWWブラウザ3から電子メールの送信データがhttpd6に送られる場合、送信される電子メールはWWWブラウザ3とhttpd6との間において、httpsにより暗号化されて転送される。

【0034】httpd6はこの送信された電子メールをCGI5を介してメール送信プログラム4に出力する。電子メールを受信したメール送信プログラム4は、通常のsmtpプロトコルにより電子メールをメールサーバ1に送信する。

【0035】従って、この電子メールの暗号化方法によれば、WWWブラウザ3とhttpd6との間における電子メールの送受信が、httpsにより暗号化された電子メールを用いて行われているため、ネットワーク上における電子メールの秘密保持を適切に行えとと共に、暗号化を行う際に、端末に暗号化のための特別な部材を設ける必要が無いため、端末のコストの上昇を抑えることができる。

【0036】次に、図1に示される電子メールの暗号化システムにおけるWWWブラウザ3の画面表示の一例を図2を参照して説明する。

【0037】図2に、図1に示されるWWWブラウザ3による画面表示の一例を示す。ただし、図1に示す電子

メールの暗号化システムと同様な部材には同じ番号を付す。この図2に示されるように、WWWブラウザ3からWWWサーバ2にアクセスし、電子メール送受信用のパスワード入力画面21をWWWブラウザ3に表示する。この画面にはCGIに備えられた送受信用のプログラムとやり取りする項目が記述されている。ここでメールサーバ1のユーザー名とパスワードを入力すると、図1に示されるCGI5の制御により、電子メール受送信選択の画面23が表示される。

【0038】電子メール受信を選択すると、電子メール一覧の画面25が表示され、メールサーバ1に届いている電子メールのタイトルの一覧を見ることができる。この画面で閲覧したい電子メールのタイトルを選択すると、電子メール受信・閲覧の画面27においてメールの内容を見ることができる。

【0039】受送信選択の画面で電子メール送信を選択すると、電子メール送信の画面29が表示され、電子メールを記入しWWWサーバ2に送信するための情報が入力できる。

【0040】WWWサーバ2とWWWブラウザ3との間の通信はすべてhttpsにより暗号化されているので、画面に表示される情報、入力する情報は暗号化されてWWWサーバ2に届く。WWWサーバ2とメールサーバ1との間は通常のpop、smtpによりデータが流れるが、メールサーバ1とhttpd6とが同一のコンピュータ上にあるため、電子メールがネットワーク上を流れることはなく、その安全性についての問題は無い。

【0041】従って、この電子メールの暗号化方法の一実施形態によれば、WWWブラウザ3を備えた端末が電子メールの受信を行う場合には、その受信する電子メールがhttpsにより暗号化され、さらに、WWWブラウザ3を備えた端末からメールサーバに電子メールの送信を行う場合には、WWWブラウザ3により暗号化されていることにより、その電子メールのセキュリティを向上させることができ、暗号化及び復号化における特別の部材も、各端末において必要ではないことから、端末のコストの上昇も抑えることができる。

【0042】次に本発明に係る電子メールの暗号化システムの実施形態について図面を参照してさらに詳細に説明する。図3に、本発明に係る電子メールの暗号化システムの一実施形態の概略図を示す。

【0043】この図3に示されるように、この電子メールの暗号化システムは、企業内ネットワーク（イントラネット）39と、企業の外、つまり社外のネットワーク（インターネット）上の端末37との間において電子メールをやり取りする場合を想定している。

【0044】企業内ネットワーク39は、受信した電子メールを蓄積するメールサーバ31と、WWWサーバ33と、外部からの不必要なデータの進入を阻止するfi

rewall35とから構成されている。

【0045】企業内ネットワーク39はfirewall35により守られており、従って、この内部での通常の電子メールの送受信は暗号化されていない。しかしながら社外のネットワークに電子メールのデータが流れるときは、暗号化を行う。

【0046】この場合、firewall35は、社外からWWWサーバ33のみはアクセスできるように設定されている。このことにより、WWWサーバ33と社外の端末37とは通信を行える。

【0047】WWWサーバ33は市販のhttps（SSL）を用いた暗号化サーバであり、社外の端末37との間の通信は、すべてhttpsにより暗号化される。また、WWWサーバ33にはメールサーバ31との間で電子メールを送受信するCGIプログラムが組み込まれている。

【0048】この図3に示される電子メールの暗号化システムの動作について詳細に説明する。図3を参照すると、社外の端末37からメールサーバ31に蓄積されている電子メールを受信するためには、まず社外の端末37に組み込まれているWWWブラウザ（不図示）を利用してWWWサーバ33にアクセスする。

【0049】WWWサーバ33には電子メールを受信したことを示す画面があり、社外の端末37上のWWWブラウザからメールサーバ31のユーザー名およびパスワードを入力すればCGIプログラムを介してメールサーバ31上の電子メールが表示される。

【0050】その際、メールサーバ31とWWWサーバ33との間は電子メールが暗号化されずに転送されるが、WWWサーバ33と社外の端末37との間はhttps（SSL）により、暗号化されて転送される。

【0051】逆に、社外の端末37からメールサーバ31に対して電子メールを送信する場合は、WWWサーバ33の電子メール送信画面上に社外の端末37のWWWブラウザから電子メールの内容を入力する。すると、WWWサーバ33はCGIプログラムを介して入力された電子メールをメールサーバ31に送信する。この際、社外の端末37からWWWサーバ33までの間は、電子メールの内容はhttpsにより暗号化されて転送される。

【0052】従って、この実施形態によれば、社外ネットワークに接続された社外の端末37において、メールサーバ31に蓄積された電子メールの送受信を行う場合、httpsにより暗号化された電子メールを用いて、WWWサーバ33と社外の端末37との間において電子メールのやり取りを行っているため、安全に電子メールの送受信を行うことができる。

【0053】また、電子メールの暗号化及び復号化は、WWWサーバ33、又は社外の端末37に備えられたWWWブラウザにより行われており、特にWWWブラウザ

は、httpsに対応したものであるならば一般的なものを利用することができるため、電子メールを暗号化及び復号化するために特別な部材を特に設ける必要はないため、社外の端末37のコストの上昇を抑えて電子メールの暗号化及び復号化を行うことができる。

【0054】また、社外の端末37は、httpsに対応したWWWブラウザを備えていれさえすれば良いため、社外ネットワーク上の任意の位置から、暗号化された電子メールの送受信を行うことができる。

【0055】

【発明の効果】以上の説明から明らかなように、本発明によれば、World Wide Webにおいて採用されているhttps(SSL)という暗号化通信の技術を用いることにより、WWWサーバとWWWブラウザとの間の全ての通信におけるデータを暗号化しているため、送受信を行う個人の特定、若しくは端末の特定を行わずに、電子メールを暗号化して送受信でき、ネットワーク上の任意の場所から、専用のソフトウェアを用いずに暗号化された電子メールを送受信することができ、その安全性と、効率を向上することの可能な電子メールの暗号化システム及び暗号化方法を提供することができる。

【0056】また、暗号化はWWWサーバとWWWブラウザ各々における情報とを使用して行うため、電子メールの暗号化のための個人、若しくは個々の端末の情報は不要である。そのため、鍵の公開等が不要であり、電子メールの暗号化を効率的に行うことが可能な電子メールの暗号化システム及び暗号化方法を提供することができ

る。

【図面の簡単な説明】

【図1】本発明に係る電子メールの暗号化システムの一実施形態の概念図である。

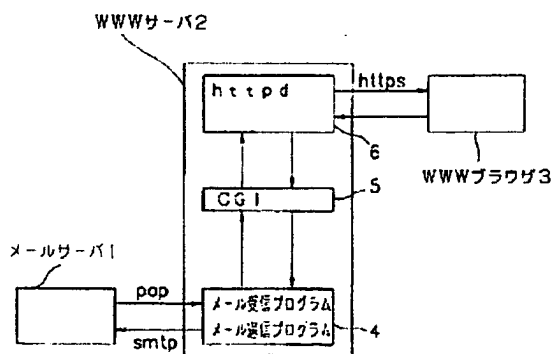
【図2】図1に示す電子メールの暗号化システムにおけるWWWブラウザによる表示画面の一例を示す図である。

【図3】本発明に係る電子メールの暗号化システムの一実施形態の概略図である。

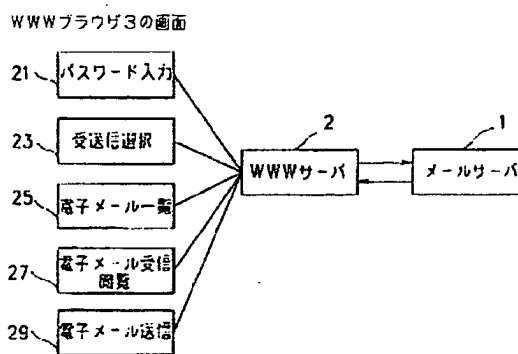
【符号の説明】

- 1 メールサーバ
- 2 WWWサーバ
- 3 WWWブラウザ
- 4 メール受信プログラム及びメール送信プログラム
- 5 CGI (Common Gateway Interface)
- 6 httpd
- 21 パスワード入力画面
- 23 受送信選択画面
- 25 電子メール一覧画面
- 27 電子メール受信・閲覧画面
- 29 電子メール送信画面
- 31 メールサーバ
- 33 WWWサーバ
- 35 firewall
- 37 社外の端末
- 39 企業内ネットワーク

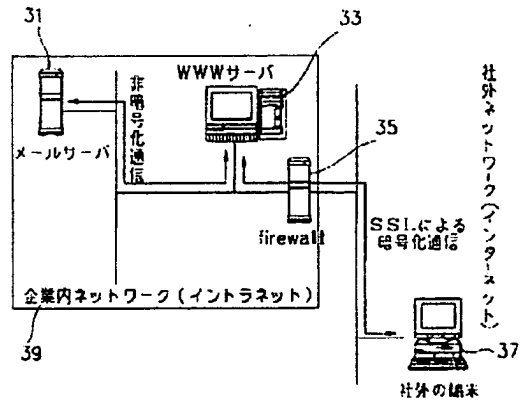
【図1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl.⁶

識別記号

F I

H 0 4 L 12/58